Efficient high-capacity quantum secret sharing with two-photon entanglement*

Fu-Guo Deng,[1,2,3,4] Xi-Han Li,[1,2,3] and Hong-Yu Zhou[1,2,3]
[1] *The Key Laboratory of Beam Technology and Material Modification of Ministry of Education, Beijing Normal University, Beijing 100875, People's Republic of China*
[2] *Institute of Low Energy Nuclear Physics, and Department of Material Science and Engineering, Beijing Normal University, Beijing 100875, People's Republic of China*
[3] *Beijing Radiation Center, Beijing 100875, People's Republic of China*
[4] *Department of Physics, Applied Optics Beijing Area Major Laboratory, Beijing Normal University, Beijing 100875, People's Republic of China*
(Dated: April 28, 2008)

An efficient high-capacity quantum secret sharing scheme is proposed following some ideas in quantum dense coding with two-photon entanglement. The message sender, Alice prepares and measures the two-photon entangled states, and the two agents, Bob and Charlie code their information on their photons with four local unitary operations, which makes this scheme more convenient for the agents than others. This scheme has a high intrinsic efficiency for qubits and a high capacity.

PACS numbers: 03.67.Dd; 03.67.Hk; 03.65.Ud; 89.70.+c

Quantum entanglement offers some novel ways for information processing and transmitting securely [1], such as quantum computation [1], quantum teleportation [2], quantum key distribution (QKD) [3, 4, 5, 6, 7], quantum dense coding [8], quantum secure direct communication (QSDC) [9, 10], and so on. A surprising property of an entangled quantum system is its nonlocality. Two parts of the quantum system cannot be considered to be independent even if they are far apart, and the single-particle measurements on these two parts cannot give all the information about the state of the whole quantum system. Quantum nonlocality has been embodied in the process of quantum teleportation [2], an important quantum technique. Ekert exploited the nonlocality feature to design a QKD protocol [3] in 1991, and Bennett, Brassard and Mermin (BBM92) [4] simplified its error rate analysis process in 1992. Also, quantum nonlocality has been used to transmit a secret message directly [9, 10].

Secret sharing is a classical cryptographic scheme [11, 12, 13] in which a boss, say Alice suspects that one of her two remote agents, say Bob and Charlie, may be dishonest but she does not know who the dishonest one is. She believes that the honest agent can prevent the dishonest one from destroying her benefits if they act in concert. For the security of her message M_A, Alice splits it into two pieces M_B and M_C, and sends them to Bob and Charlie, respectively. The two agents can read out the message $M_A = M_B \oplus M_C$ only when they cooperate. As a classical signal can be copied perfectly, it is impossible to create a private key with classical physics. When quantum mechanics enters the field of information, the story is changed. Quantum secret sharing (QSS) is the generalization of classical secret sharing into quantum scenario and has progressed quickly in recent years [14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33].

One of the main goals of QSS, similar to QKD, is to distribute the private keys among the three participants, or more generally, many participants securely [14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26]. An original QSS scheme was proposed by Hillery, Bužek and Berthiaume [14] in 1999, which is called HBB99 hereafter. In the HBB99 scheme [14], the secret sharing is accomplished by using a three-photon entangled Greenberger-Horne-Zeilinger (GHZ) state. Each participant holds a photon from a GHZ state, and chooses randomly one measuring-basis (MB) from the X-MB and the Y-MB to measure their photons independently, similar to BBM92 QKD scheme [4]. Subsequently Karlsson, Koashi and Imoto (KKI) put forward another QSS scheme [15] with a two-photon polarization-entangled state. The photons are polarized along the z or x directions, and the two agents measure their photons choosing randomly one of the two MBs, Z and X. The efficiency for qubits $\eta_q \equiv \frac{q_u}{q_t}$ in these two protocols [14, 15] is 50% because half of the instances are discarded as the participants choose incompatible MBs, similar to the BBM92 QKD protocol [4]. Here q_u is the useful qubits and q_t is the total qubits transmitted [6, 34]. Each entangled quantum system can be used to carry on average a half bit of the random common key, and two or more bits of classical communications are required to compare the correlation of their MBs. Their total efficiency η_t is low; η is defined as [6, 34]

$$\eta_t = \frac{b_s}{q_t + b_t}, \tag{1}$$

where b_s, q_t and b_t are the number of bits in the raw key, the qubits transmitted, and the total classical bits exchanged between the participants in the quantum communication, respectively. For instance, the total efficiency in HBB99 QSS scheme [14] with three parties is at most $\eta_t = \frac{0.5}{2+2} = 12.5\%$ as the three parties transmit a two-qubit (i.e., two particles in a three-particle GHZ state) quantum system to create half bit of key

*Published in *Phys. Lett.* A 372 (2008) 1957

at the expense of exchanging at least two bits of classical information about their MBs. That is, Alice and Bob (or Charlie) exchange a bit of information about Bob's (Charlie's) MB, i.e., $b_t = 2$. In KKI QSS scheme [15] with three parties, the parties use a two-qubit quantum system to obtain half bit of key in principle, i.e., its total efficiency is at most $\eta_t = \frac{0.5}{2+2} = 12.5\%$.

In this Letter, we present an efficient high-capacity QSS scheme for distributing a random key among three participants with a two-photon entangled state based on quantum dense coding. The two agents, Bob and Charlie choose the single-photon measurements on the sampling photons with the three MBs Z, X and Y randomly for eavesdropping check, and encode their information with four local unitary operations on their photons. Almost all the entangled states can be used to exchange the random key and each two-photon entangled state can carry two bits of information. Moreover, this scheme is secure with the decoy photons and the classical information exchanged is reduced largely as the participants almost need not compare their MBs for all the instances except for those for eavesdropping check. The efficiency for qubits η_q approaches 1 and the total efficiency η_t approaches 50% (neglecting the instances for checking eavesdropping, same as those in other QSS schemes) as the two qubits are transmitted double the distance between the sender Alice and her agents, which equals four qubits are transmitted in the KKI QSS scheme, and two bits of key are created in theory.

An Einstein-Podolsky-Rosen (EPR) pair is in one of the four Bell states shown as follows.

$$\begin{aligned}
|\phi^+\rangle &= \frac{1}{\sqrt{2}}(|+z\rangle_B|+z\rangle_C + |-z\rangle_B|-z\rangle_C) \\
&= \frac{1}{\sqrt{2}}(|+x\rangle_B|+x\rangle_C + |-x\rangle_B|-x\rangle_C) \\
&= \frac{1}{\sqrt{2}}(|+y\rangle_B|-y\rangle_C + |-y\rangle_B|+y\rangle_C), \\
|\phi^-\rangle &= \frac{1}{\sqrt{2}}(|+z\rangle_B|+z\rangle_C - |-z\rangle_B|-z\rangle_C) \\
&= \frac{1}{\sqrt{2}}(|+x\rangle_B|-x\rangle_C + |-x\rangle_B|+x\rangle_C) \\
&= \frac{1}{\sqrt{2}}(|+y\rangle_B|+y\rangle_C + |-y\rangle_B|-y\rangle_C), \\
|\psi^+\rangle &= \frac{1}{\sqrt{2}}(|+z\rangle_B|-z\rangle_C + |-z\rangle_B|+z\rangle_C) \\
&= \frac{1}{\sqrt{2}}(|+x\rangle_B|+x\rangle_C - |-x\rangle_B|-x\rangle_C) \\
&= \frac{-i}{\sqrt{2}}(|+y\rangle_B|+y\rangle_C - |-y\rangle_B|-y\rangle_C), \\
|\psi^-\rangle &= \frac{1}{\sqrt{2}}(|+z\rangle_B|-z\rangle_C - |-z\rangle_B|+z\rangle_C) \\
&= \frac{1}{\sqrt{2}}(|-x\rangle_B|+x\rangle_C - |+x\rangle_B|-x\rangle_C) \\
&= \frac{i}{\sqrt{2}}(|+y\rangle_B|-y\rangle_C - |-y\rangle_B|+y\rangle_C), \quad (2)
\end{aligned}$$

where $|+z\rangle \equiv |0\rangle$ and $|-z\rangle \equiv |1\rangle$ are the eigenvectors of the MB Z (for example the polarizations of a photon along the z-direction), and $|+x\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-x\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ are those of the MB X. The subscripts B and C indicate the two correlated photons in each Einstein-Podolsky-Rosen (EPR) pair. The four local unitary operations U_i $(i = 0, 1, 2, 3)$ can transform one of the Bell states into another,

$$\begin{aligned}
U_0 &\equiv I = |0\rangle\langle 0| + |1\rangle\langle 1|, \\
U_1 &\equiv \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|, \\
U_2 &\equiv \sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|, \\
U_3 &\equiv i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|, \quad (3)
\end{aligned}$$

where I is the 2×2 identity matrix and σ_i $(i = x, y, z)$ are the Pauli matrices, i.e.,

$$\begin{aligned}
&I \otimes U_0|\psi^\pm\rangle = |\psi^\pm\rangle, \quad && I \otimes U_0|\phi^\pm\rangle = |\phi^\pm\rangle, \\
&I \otimes U_1|\psi^\pm\rangle = -|\psi^\mp\rangle, && I \otimes U_1|\phi^\pm\rangle = |\phi^\mp\rangle, \\
&I \otimes U_2|\psi^\pm\rangle = |\phi^\pm\rangle, && I \otimes U_2|\phi^\pm\rangle = |\psi^\pm\rangle, \\
&I \otimes U_3|\psi^\pm\rangle = |\phi^\mp\rangle, && I \otimes U_3|\phi^\pm\rangle = -|\psi^\mp\rangle. \quad (4)
\end{aligned}$$

The four Bell states can be used to carry two bits of classical information [8, 9], but we cannot send the photon pair directly into an insecure channel as the four Bell states are the the simultaneous eigenvectors of the two-body operators $\{\sigma_z^{(B)}\sigma_z^{(C)}, \sigma_x^{(B)}\sigma_x^{(C)}\}$ and they can be copied freely, which renders the transmission insecure. To prevent an eavesdropper Eve from eavesdropping, one way is not allowing Eve to acquire simultaneously both photons in each EPR pair, such as those in the two-step quantum communication scheme [6, 9] and its variant [10]. Another method is to change the order of a group of EPR pairs with two quantum channels so as to confuse Eve the correct matching of the photons in the group of EPR pairs, for instance that in the controlled-order-rearrangement-encryption technique for QKD [7].

In QSS, if the participants can prevent the dishonest agent, say Bob, from eavesdropping the quantum channel freely, any eavesdropper can be found out [15]. Similar to Ref. [15], Alice can prepare each photon pair in one of the nonorthogonal entangled states, which will forbid the dishonest one to copy the quantum system without disturbing it. To the end, Alice should pick out two nonorthogonal bases to prepare the entangled photon pairs, similar to Bennet-Brassard 1984 (BB84) QKD protocol [35]. Certainly, one set of basis for an entangled photon pair is the four Bell states, shown in Eq (2). Another set of basis can be chosen as follows.

$$\begin{aligned}
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|+x\rangle_B|+z\rangle_C + i|-x\rangle_B|-z\rangle_C) \\
&= \frac{1}{\sqrt{2}}(|+z\rangle_B|+y\rangle_C + |-z\rangle_B|-y\rangle_C) \\
&= \frac{e^{\frac{-i\pi}{4}}}{\sqrt{2}}(|+y\rangle_B|-x\rangle_C + i|-y\rangle_B|+x\rangle_C),
\end{aligned}$$

$$
\begin{aligned}
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|+x\rangle_B|+z\rangle_C - i|-x\rangle_B|-z\rangle_C) \\
&= \frac{1}{\sqrt{2}}(|+z\rangle_B|-y\rangle_C + |-z\rangle_B|+y\rangle_C) \\
&= \frac{e^{\frac{-i\pi}{4}}}{\sqrt{2}}(|+y\rangle_B|+x\rangle_C + i|-y\rangle_B|-x\rangle_C), \\
|\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|+x\rangle_B|-z\rangle_C + i|-x\rangle_B|+z\rangle_C) \\
&= \frac{i}{\sqrt{2}}(|+z\rangle_B|-y\rangle_C - |-z\rangle_B|+y\rangle_C) \\
&= \frac{e^{\frac{i3\pi}{4}}}{\sqrt{2}}(|+y\rangle_B|-x\rangle_C - i|-y\rangle_B|+x\rangle_C), \\
|\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|+x\rangle_B|-z\rangle_C - i|-x\rangle_B|+z\rangle_C) \\
&= \frac{-i}{\sqrt{2}}(|+z\rangle_B|+y\rangle_C - |-z\rangle_B|-y\rangle_C) \\
&= \frac{e^{\frac{-i\pi}{4}}}{\sqrt{2}}(|+y\rangle_B|-x\rangle_C + i|-y\rangle_B|+x\rangle_C), \quad (5)
\end{aligned}
$$

where $|\pm y\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$ are the two eigenvectors of the MB Y. The four local unitary operations U_i $(i = 0, 1, 2, 3)$ can transfer one of the four entangled states $\{|\Phi^\pm\rangle, |\Psi^\pm\rangle\}$ into another, i.e.,

$$
\begin{aligned}
&I \otimes U_1|\Phi^\pm\rangle = |\Phi^\mp\rangle, \quad I \otimes U_1|\Psi^\pm\rangle = |\Psi^\mp\rangle, \\
&I \otimes U_2|\Phi^\pm\rangle = |\Psi^\pm\rangle, \quad I \otimes U_2|\Psi^\pm\rangle = |\Phi^\pm\rangle, \\
&I \otimes U_3|\Phi^\pm\rangle = -|\Psi^\mp\rangle, \quad I \otimes U_3|\Psi^\pm\rangle = |\Phi^\mp\rangle, \\
&U_1 \otimes I|\Phi^\pm\rangle = |\Psi^\mp\rangle, \quad U_1 \otimes I|\Psi^\pm\rangle = |\Phi^\mp\rangle, \\
&U_2 \otimes I|\Phi^\pm\rangle = |\Phi^\mp\rangle, \quad U_2 \otimes I|\Psi^\pm\rangle = -|\Psi^\mp\rangle, \\
&U_3 \otimes I|\Phi^\pm\rangle = |\Psi^\pm\rangle, \quad U_3 \otimes I|\Psi^\pm\rangle = -|\Phi^\pm\rangle. \quad (6)
\end{aligned}
$$

The two basis sets $\{|\phi^\pm\rangle, |\psi^\pm\rangle\}$ and $\{|\Phi^\pm\rangle, |\Psi^\pm\rangle\}$ are not orthogonal, which forbids any one to copy them perfectly, same as that in Ref. [15].

Now, let us describe the principle of our QSS scheme in detail as follows.

(1). Alice, Bob and Charlie agree that each of the four local unitary operations U_0, U_1, U_2 and U_3 represents the two-bit information.

(2). Alice prepares the two photons B and C in one of the eight nonorthogonal entangled states $\{|\phi^\pm\rangle, |\psi^\pm\rangle, |\Phi^\pm\rangle, |\Psi^\pm\rangle\}$ randomly. She sends the photon B to Bob and C to Charlie.

For preventing the dishonest agent from eavesdropping freely with an opaque attack [36], Alice sends a decoy photon [37, 38], which is randomly in one of the six states $\{|0\rangle, |1\rangle, |+x\rangle, |-x\rangle, |+y\rangle, |-y\rangle\}$, to each agent with the probability p_d (we give the reason for choosing decoy photons below). Alice can prepare the decoy photon by measuring one photon in the two-photon quantum system which is in one of the two states $\{|\phi^+\rangle, |\Phi^+\rangle\}$ with the MB σ_z [38]. Also, she can produce it with an ideal single-photon source [37, 38].

(3). Bob and Charlie choose one of the two modes, a small probability p_c $(< 1/2)$ with the checking-eavesdropping mode and a large probability $1 - p_c$ with the coding mode, for their photons received, similar to those in the Refs. [9, 10, 39].

If Bob (Charlie) chooses the checking-eavesdropping mode, Bob (Charlie) measures his photon by choosing one of the three MBs Z, X and Y randomly; otherwise, Bob (Charlie) encodes his random key on the photon received with one of the four unitary operations $\{U_i\}$ $(i = 0, 1, 2, 3)$. He sends the photon back to the sender Alice.

(4) Alice takes a Bell-basis measurement on each two correlated photons received from Bob and Charlie with the two-photon entanglement basis $\{|\phi^\pm\rangle, |\psi^\pm\rangle\}$ or $\{|\Phi^\pm\rangle, |\Psi^\pm\rangle\}$, as the same as that she prepares them before the communication.

As the operations done by the agents on the quantum system composed of the photons B and C do not change its basis, the measurement done by Alice is deterministic and will give out the outcome of the combination of the unitary operations performed by Bob and Charlie, say $U_A = U_B \otimes U_C$. Here U_B and U_C are the operations done by Bob and Charlie, respectively. If the communication is secure, each of the four unitary operations represents two bits of classical information which can be used as the raw key in QSS.

If one of the two agents, say Bob, measures his photon and the other agent (Charlie) sends his photon back to Alice, instead of encoding it, Alice will get nothing with her Bell-basis measurement.

(5). Alice tells her agents which entangled basis has been chosen for each EPR pair and completes the error rate with the helps of her two agents.

She requires Bob and Charlie to publish the MBs and the outcomes of the sample photons for which they choose the checking-eavesdropping mode. Alice exploits the refined error analysis technique [40] for checking eavesdropping of the process of the transmission from Alice to her agents. That is, Alice only picks up the decoy photons measured by the agents to check eavesdropping. As the agents measure the decoy photons with the three MBs, Z, Y and X, the probability that the outcomes of the agents' are correlated with those of Alice's is $\frac{1}{3}P_dP_c$. Similar to Ref. [40], this eavesdropping check will find out the eavesdropper monitoring the quantum channel from Alice to her agents as any eavesdropping will leave a trace in the outcomes of the decoy sampling photons.

For preventing the dishonest agent from eavesdropping the process from the other agent to Alice freely, Alice should also pick out randomly a sufficiently large subset of the outcomes from the Bell-basis measurements on the entangled quantum systems, and analyzes its error rate, named it as the second check. It is useful for check the security of the quantum channel when the photons run from the two agents back to Alice. Moreover, it can provide an estimate information for the postprocessing, such as the error correct and the privacy amplification. For half of these instances, Alice requires Bob first publish his operations and then Charlie, or vice versa.

(6). If all the error rates are low than the threshold ε_{th}, they can use the results remained as a raw key and distill a private key $K_A = K_B \oplus K_C$ with error correction and privacy amplification [5]; otherwise, they will abandon the outcomes transmitted and repeat the quantum communication from the beginning.

It is of interesting to point out the advantages that Alice replaces some photons in the Bell states with the decoy photons [37, 38]. If Alice does not exploit the decoy photons, a dishonest agent, say Bob can steal some information with an opaque attack freely and fully [36], especially when the transmission efficiencies lower than 50%. In detail, Bob intercepts the photon C when it is sent from Alice to Charlie, and stores it with a quantum memory. He prepares a fake EPR pair $B'C'$ in the state $|\phi^+\rangle_{B'C'} = \frac{1}{\sqrt{2}}(|+z\rangle_{B'}|+z\rangle_{C'} + |-z\rangle_{B'}|-z\rangle_{C'})$ and sends the photon C' to Charlie, instead of the photon C. If Charlie operates the photon C' and sends it back to Alice, Bob can capture this photon and take a Bell-state measurement on the photons $B'C'$. He can obtain all the information about the operations done by Charlie in this way. On the other hand, if Charlie measures the photon C' with the MB Z, X or Y, Bob will get no photon in the quantum signal sent from Charlie to Alice. He can determine this condition with a quantum non-demolition measurement, as same as that in Ref. [9, 39]. Subsequently, Bob can keep the photon B only when he gets the outcome $|\phi^+\rangle_{B'C}$. In this way, Bob's eavesdropping introduces no errors in the outcomes of the measurements done by Bob and Charlie (or Alice and Charlie) no matter what the MB chosen by Charlie is [36]. Certainly, Bob's eavesdropping will introduce errors in the outcomes if Bob gets the other three Bell-basis results. However, Bob can hide his eavesdropping with cheating [36]. That is, he can announce that he gets nothing when he measures the photon B as there are losses in the quantum line [36]. On the other hand, without the decoy photons, Alice should measure one EPR particle when the other EPR particle is measured by her agent. For accomplishing this task, she should first judge the photon number in each signal sent back by each agent, which will require Alice to have the capability of taking a quantum non-demolition measurement.

The process of eavesdropping check with decoy photons between Alice and Charlie does not require Bob to participate in it, which will forbid Bob eavesdrop the quantum channel from Alice to Charlie with an opaque attack strategy [36]. The same process takes place between Alice and Bob. In essence, the process of the photon transmission from Alice to her each agent is similar to the QKD protocol proposed by Lo et al. [40] which is proven to be secure. That is, this process can be made to be secure, same as QKD [35, 40].

After the operations done by the agents, the density matrix of the quantum system composed of the photons B and C is $\rho_{BC} = \begin{pmatrix} 1/4 & 0 & 0 & 0 \\ 0 & 1/4 & 0 & 0 \\ 0 & 0 & 1/4 & 0 \\ 0 & 0 & 0 & 1/4 \end{pmatrix}$ for the dishonest agent, and he cannot copy the quantum signal freely, similar to BB84 [35] and BBM92 [4] QKD protocols. So this QSS scheme can be made to be secure, which is in principle different from the QSS schemes [14, 15, 16, 17, 18, 19, 20, 21, 22] in which the process of checking eavesdropping is completed with the cooperation of the dishonest agent. On the other hand, as the security of the process of the transmission from Alice to her agents is ensured with the decoy photons and that from the agents to Alice is ensured with the samples of the outcomes obtained with Bell-basis measurements, this QSS scheme does not require the participants to have the capability of storing quantum states. As for the multi-photon attack [21], the agents can use a filter to prevent a fake photon with a nonstandard wavelength from entering their devices and use some beam splitters to split the sampling signals chosen for eavesdropping check before they measure the signals with the MB Z, X or Y, same as that in Ref. [41]. Also, the parties can complete a faithful qubit transmission against collective noise with the technique in Ref. [42], which will improve the practical efficiency in this QSS scheme.

Without the decoy photons prepared by Alice, this QSS scheme can be made secure if both Bob and Charlie have an ideal single-photon source. In detail, when Bob (Charlie) chooses the checking-eavesdropping mode, he measures the photon B (C) sent by Alice with one of the three bases Z, X, and Y, and then sends a photon prepared by himself to Alice. This photon can be randomly in one of the six states $\{|\pm z\rangle, |\pm x\rangle, |\pm y\rangle\}$. In this way, the eavesdropper does not know which is the sample photon before Alice receives the entangled EPR pair, and the opaque attack can be overcome as Alice can use the photons inserted by her agents to check the security of the transmission of photons from the agents to Alice. In essence, the honest agent prepares the decoy photons and uses them to prevent the potentially dishonest agent from eavesdropping freely.

In fact, this QSS scheme is the modified version of the KKI QSS scheme [15] with quantum dense coding and decoy photons. But only those modifications increase its intrinsic efficiency, the source capacity and the security largely. Almost all the instances ($(1-P_d)(1-P_c)^2$) are useful for generating the raw key except for those chosen for eavesdropping check, and each of the two-photon entangled quantum system can carry two bits of information. Moreover, the classical information exchanged is reduced largely as the two agents need not publish their MBs when they choose the coding mode with the four local unitary operations. Then the efficiency for qubits $\eta_q = (1-P_d)(1-P_c)^2$ approaches 1 when P_d and P_c are very small. As the two qubits in the entangled states are transmitted double the distances between the sender Alice and her agents, which equals to that

Alice and her agents transmit four qubits, the total efficiency $\eta_t = \frac{2}{4}\frac{(1-P_d)(1-P_c)^2}{1+P_c}$ in the present QSS scheme, approaching 50% when P_d and P_c are very small. Certainly, in a practical application with a noisy quantum channel, the efficiency for qubits cannot approach 1 and the total efficiency is low than 50% as the probabilities P_d and P_c cannot be arbitrarily small. The parties can exploit error-avoiding codes to reduce the effect of noise on the efficiencies, such as the faithful qubit transmission technique with linear optics [42].

In summary, we introduce an efficient high-capacity QSS scheme with quantum dense coding based on two-photon entangled states. The two agents, Bob and Charlie choose the single-photon measurements on the sampling photons with the three MBs randomly for eavesdropping check, and encode their information with four local unitary operations, which make this QSS scheme more convenient for the agents than some others [14, 15]. Almost all the entangled photon pairs can be used to exchange the random key and each photon pair can carry two bit of information. The intrinsic efficiency for qubit is double as that in KKI QSS scheme [15], and the source capacity is four times as the latter with the photons running forth and back. Moreover, this scheme is secure with decoy photons and the classical information exchanged is reduced largely as the participants almost need not compare their MBs for all the instances except for those for eavesdropping check. As the efficiency for producing three-particle entangled state is low than that for two-particle entangled state, the present QSS scheme is more practical with present technology than the first one proposed by Hillery, Bužek, and Berthiaume [14].

[1] M.A. Nielsen, I.L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, UK, 2000).
[2] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W.K. Wootters, Phys. Rev. Lett. 70 (1993) 1895.
[3] A.K. Ekert, Phys. Rev. Lett. 67 (1991) 661.
[4] C.H. Bennett, G. Brassard, N.D. Mermin, Phys. Rev. Lett. 68 (1992) 557.
[5] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. 74 (2002) 145.
[6] G.L. Long, X.S. Liu, Phys. Rev. A 65 (2002) 032302.
[7] F.G. Deng, G. L. Long, Phys. Rev. A 68 (2003) 042315.
[8] C.H. Bennett, S.J. Wiesner, Phys. Rev. Lett. 69 (1992) 2881; X.S. Liu et al., Phys. Rev. A 65 (2002) 022304.
[9] F.G. Deng et al., Phys. Rev. A 68 (2003) 042317; Phys. Lett. A 359 (2006) 359; Phys. Scr. 76 (2007) 25.
[10] C. Wang et al., Phys. Rev. A 71 (2005) 044305; Opt. Commun. 253 (2005) 15; X.H. Li et al., Chin. Phys. 16 (2007) 2149.
[11] G.R. Blakley, in *Proceedings of the American Federation of Information Processing 1979 National Computer Conference* (American Federation of Information Processing, Arlington, VA, 1979), pp.313-317;
[12] A. Shamir, Commun. ACM **22**, 612 (1979);
[13] B. Schneier, *Applied Crytography* (Wiley, New York, 1996), p.70; see also J. Gruska, *Foundations of Computing* (Thomson Computer Press, London, 1997), p.504.
[14] M. Hillery, V. Bužek, A. Berthiaume, Phys. Rev. A 59 (1999) 1829.
[15] A. Karlsson, M. Koashi, N. Imoto, Phys. Rev. A 59 (1999) 162.
[16] S. Bandyopadhyay, Phys. Rev. A 62 (2000) 012308.
[17] V. Karimipour, A. Bahraminasab, S. Bagherinezhad, Phys. Rev. A 65 (2002) 042320.
[18] F.G. Deng et al., Phys. Lett. A 337 (2005) 329; Phys. Lett. A 340 (2005) 43; Phys. Lett. A 354 (2006) 190; J. Phys. A 39 (2006) 14089; Chin. Phys. Lett. 21 (2004) 2097; Chin. Phys. Lett. 23 (2006) 1084.
[19] L. Xiao et al., Phys. Rev. A 69 (2004) 052307.
[20] Z.J. Zhang et al., Phys. Rev. A 71 (2005) 044301.
[21] F.G. Deng et al., Phys. Rev. A 72 (2005) 044302.
[22] F.L. Yan, T. Gao, Phys. Rev. A 72 (2005) 012304.
[23] G.P. Guo, G.C. Guo, Phys. Lett. A 310 (2003) 247.
[24] Z.J. Zhang, Z.X. Man, Phys. Rev. A 72 (2005) 022303.
[25] P. Zhou et al., Physica A 381 (2007) 164; Chin. Phys. Lett. 24 (2007) 2181.
[26] P. Chen et al., Chin. Phys. 15 (2006) 2228; Prog. Natural Sci. 17 (2007) 26.
[27] R. Cleve, D. Gottesman, H.K. Lo, Phys. Rev. Lett. 83 (1999) 648.
[28] Y.M. Li, K.S. Zhang, K.C. Peng, Phys. Lett. A 324 (2004) 420.
[29] F.G. Deng et al., Phys. Rev. A 72 (2005) 044301; Eur. Phys. J. D 39 (2006) 459.
[30] F.G. Deng et al., Phys. Rev. A 72 (2005) 022338.
[31] X.H. Li et al., J. Phys. B 39 (2006) 1975; Chin. Phys. Lett. 24 (2007) 1151; P. Zhou et al., J. Phys. A 40 (2007) 13121.
[32] W. Tittel, H. Zbinden, N. Gisin, Phys. Rev. A 63 (2001) 042301.
[33] A.M. Lance et al., Phys. Rev. Lett. 92 (2004) 177903.
[34] A. Cabello, Phys. Rev. Lett. 85 (2000) 5635.
[35] C.H. Bennett, G. Brassad, *Proc. IEEE Int.Conf. on Computers, Systems and Signal Processing, Bangalore*, India (IEEE, New York, 1984), P175-179.
[36] F.G. Deng, X. H. Li, H. Y. Zhou, arxiv: 0705.0279.
[37] C.Y. Li et al., Chin. Phys. Lett. 22 (2005) 1049 ; Chin. Phys. Lett. 23 (2006) 2896.
[38] X.H. Li et al., J. Korean Phys. Soc. 49 (2006) 1353.
[39] F.G. Deng, G.L. Long, Phys. Rev. A 69 (2004) 052319; Phys. Rev. A 70 (2004) 012311; Commun. Theor. Phys. 46 (2006) 443.
[40] H.K. Lo, H.F. Chau, M. Ardehali, J. Cryptology 18 (2005) 133.
[41] X.H. Li, F.G. Deng, H.Y. Zhou, Phys. Rev. A 74 (2006) 054302.
[42] X.H. Li, F.G. Deng, H.Y. Zhou, Appl. Phys. Lett. 91 (2007) 144101.